INOMATEC: Jurnal Inovasi dan Kajian Multidisipliner Kontemporer
Vol. 01, No. 03, Tahun 2026, Hal. 300-305, ISSN: 3123-5573 (Online)

Studi Keamanan Jaringan *Wireless* terhadap Serangan *Man-In-The-Middle* (MITM)

Rakhamdi Rahman[1], Muhammad Vickram Islamy Fahrezy[2], Ahmad Ridhotullah[3]
[1,2,3] Institut Teknologi Bacharuddin Jusuf Habibie Parepare
rakhmadi.rahman@ith.ac.id[1], muhammadvikram114@gmail.com[2], ahmadridhotullah2006@gmail.com[3]

Article Info
Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Keywords:
wireless network, network security, Man-in-the-Middle, MITM, CIA Triad.

ABSTRACT
The use of wireless networks as a data communication medium continues to increase along with the development of information technology and the need for user mobility. Although offering flexibility and ease of implementation, wireless networks have a higher level of security vulnerabilities than wired networks, particularly against Man-in-the-Middle (MITM) attacks. This attack allows attackers to intercept, monitor, and manipulate data traffic without the knowledge of the communicating parties, thus threatening the Confidentiality, Integrity, and Availability Triad (CIA Triad). This study aims to assess the security of wireless networks against MITM attacks through a qualitative approach based on a Systematic Literature Review (SLR). The review process was conducted in accordance with PRISMA guidelines to ensure a systematic and transparent literature analysis. The analysis focused on identifying wireless network characteristics, MITM attack techniques, and security mechanisms that can be implemented to minimize the risk of attacks. The study results show that wireless networks with minimal security are highly vulnerable to MITM attacks. The implementation of security mechanisms such as strong encryption, secure authentication, and layered network monitoring has been shown to significantly improve network protection. The combination of these mechanisms not only reduces the potential for data eavesdropping and manipulation but also increases system reliability and user confidence in the security of wireless networks.

Article Info
Article history:
Received December 29, 2025
Revised December 31, 2025
Accepted January 04, 2026

Kata Kunci:
jaringan wireless, keamanan jaringan, *Man-in-the-Middle*, MITM, CIA Triad.

ABSTRAK
Penggunaan jaringan wireless sebagai media komunikasi data terus meningkat seiring dengan perkembangan teknologi informasi dan kebutuhan mobilitas pengguna. Meskipun menawarkan fleksibilitas dan kemudahan implementasi, jaringan wireless memiliki tingkat kerentanan keamanan yang lebih tinggi dibandingkan jaringan berbasis kabel, khususnya terhadap serangan *Man-in-the-Middle* (MITM). Serangan ini memungkinkan penyerang untuk mengintersepsi, memantau, dan memanipulasi lalu lintas data tanpa disadari oleh pihak yang berkomunikasi, sehingga mengancam aspek *Confidentiality*, *Integrity*, dan *Availability* (CIA Triad). Penelitian ini bertujuan untuk mengkaji keamanan jaringan wireless terhadap serangan MITM melalui pendekatan kualitatif berbasis *Systematic Literature Review* (SLR). Proses kajian dilakukan dengan mengacu pada pedoman PRISMA untuk memastikan analisis literatur yang sistematis dan transparan. Analisis difokuskan pada identifikasi karakteristik jaringan wireless, teknik serangan MITM, serta mekanisme keamanan yang dapat diterapkan untuk meminimalkan risiko serangan. Hasil kajian menunjukkan bahwa jaringan wireless dengan tingkat pengamanan minimal sangat rentan terhadap

serangan MITM. Penerapan mekanisme keamanan berupa enkripsi yang kuat, autentikasi yang aman, serta monitoring jaringan secara berlapis terbukti mampu meningkatkan perlindungan jaringan secara signifikan. Kombinasi mekanisme tersebut tidak hanya mengurangi potensi penyadapan dan manipulasi data, tetapi juga meningkatkan keandalan sistem dan kepercayaan pengguna terhadap keamanan jaringan wireless.

Corresponding Author:
Rakhmadi Rahman
Sistem Informasi Institut Teknologi Bacharuddin Jusuf Habibie Parepare
E-mail: rakhmadi.rahman@ith.ac.id

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi saat ini sangat mendorong kenaikan dalam penggunaan jaringan *wireless* sebagai media utama dalam pertukaran data digital. Jaringan *wireless* banyak dipilih karena fleksibilitas, kemudahan instalasi, serta dukungan mobilitas tinggi, sehingga digunakan secara luas di berbagai lingkungan, baik pada lingkungan pendidikan, perkantoran, dan fasilitas publik. Namun, karakteristik transmisi data melalui media udara yang bersifat terbuka menjadikan jaringan *wireless* memiliki tingkat kerentanan keamanan yang lebih tinggi dibandingkan jaringan kabel. Sifat broadcast pada jaringan *wireless* memungkinkan pihak yang tidak berwenang untuk mengakses jaringan selama berada dalam jangkauan sinyal. Kondisi ini meningkatkan risiko terjadinya berbagai serangan siber, khususnya serangan penyadapan dan manipulasi data. Salah satu ancaman paling serius pada jaringan *wireless* adalah serangan *Man-in-the-Middle* (MITM), yaitu serangan yang terjadi ketika penyerang berada di antara dua pihak yang berkomunikasi tanpa sepengetahuan keduanya. Melalui serangan ini, penyerang dapat memantau, mencuri, bahkan memodifikasi data yang ditransmisikan.

Serangan MITM umumnya memanfaatkan kelemahan pada mekanisme autentikasi dan enkripsi. Teknik yang sering digunakan meliputi evil twin attack, ARP spoofing, dan packet sniffing, yang memungkinkan penyerang mengalihkan lalu lintas data melalui perangkatnya. Serangan tersebut sulit dideteksi oleh pengguna karena komunikasi tetap berlangsung secara normal. Dampak yang ditimbulkan dapat berupa pencurian informasi sensitif, seperti kredensial pengguna dan data pribadi, serta kebocoran data penting milik organisasi yang berpotensi menimbulkan kerugian finansial dan menurunkan reputasi. Keamanan jaringan wireless berperan penting dalam menjaga aspek kerahasiaan, integritas, dan ketersediaan informasi. Oleh karena itu, diperlukan penerapan sistem keamanan yang komprehensif untuk meminimalkan risiko serangan MITM. Penggunaan enkripsi yang kuat seperti WPA2 dan WPA3, mekanisme autentikasi yang aman, serta monitoring jaringan secara berkelanjutan merupakan langkah penting dalam meningkatkan perlindungan jaringan wireless. Dengan penerapan sistem keamanan yang tepat, pemanfaatan jaringan wireless dapat berlangsung secara aman dan berkelanjutan.

TINJAUAN PUSTAKA

a. Jaringan *Wireless* dan Karakteristik Keamanannya

Jaringan *wireless* memanfaatkan gelombang radio sebagai media transmisi utama untuk menghubungkan perangkat tanpa memerlukan media fisik seperti kabel. Karakteristik ini memberikan fleksibilitas tinggi serta mendukung mobilitas pengguna dalam area cakupan tertentu. Namun, sifat transmisi yang terbuka menyebabkan sinyal *wireless* dapat diterima oleh berbagai pihak yang berada dalam jangkauan, sehingga meningkatkan potensi ancaman keamanan dibandingkan jaringan berbasis kabel. Keamanan jaringan secara konseptual mengacu pada *CIA Triad*, yang terdiri dari *Confidentiality*, *Integrity*, dan *Availability* sebagai prinsip dasar perlindungan informasi. *Confidentiality* berfokus pada pembatasan akses data hanya kepada pihak yang berwenang, *Integrity* menjamin keutuhan data selama proses penyimpanan dan transmisi, sedangkan *Availability* memastikan sistem dan layanan jaringan tetap dapat diakses saat dibutuhkan. Ketiga hal ini saling terhubung dan melahirkan landasan utama dalam perancangan sistem keamanan jaringan yang efektif.

b. Serangan Man-in-the-Middle pada Jaringan Wireless

Serangan *Man-in-the-Middle* (MITM) merupakan salah satu ancaman siber yang secara langsung mengganggu prinsip *Confidentiality* dan *Integrity* dalam keamanan jaringan. Serangan ini terjadi ketika penyerang berhasil memposisikan dirinya di antara dua entitas yang sedang berkomunikasi tanpa disadari oleh kedua pihak tersebut. Dalam situasi ini, penyerang memiliki kemampuan untuk memantau lalu lintas komunikasi secara real-time serta melakukan manipulasi terhadap data yang dikirimkan. Pada jaringan wireless, serangan MITM umumnya memanfaatkan kelemahan pada protokol komunikasi dan mekanisme autentikasi. Beberapa teknik yang sering digunakan antara lain *ARP spoofing* untuk mengalihkan lalu lintas data, *Evil Twin attack* dengan membuat access point palsu yang menyerupai jaringan resmi, *DNS spoofing* untuk mengarahkan pengguna ke situs berbahaya, serta *SSL stripping* yang menurunkan tingkat keamanan komunikasi terenkripsi. Teknik-teknik tersebut menjadikan serangan MITM sulit dideteksi oleh pengguna karena komunikasi tetap berlangsung secara normal.

c. Dampak Serangan MITM terhadap Keamanan Jaringan

Serangan MITM pada jaringan *wireless* dapat menimbulkan dampak signifikan bagi pengguna individu maupun organisasi. Informasi sensitif seperti kredensial autentikasi, data pribadi, dan informasi keuangan berisiko dicuri tanpa sepengetahuan korban. Dalam konteks organisasi, serangan ini berpotensi menyebabkan kebocoran data rahasia, gangguan layanan sistem informasi, serta menurunnya tingkat kepercayaan pengguna terhadap keamanan jaringan. Oleh karena itu, pemahaman terhadap karakteristik jaringan wireless dan teknik serangan MITM menjadi aspek penting dalam upaya meningkatkan perlindungan keamanan jaringan.

METODE ANALISIS DATA

Analisis data dalam penelitian ini dilakukan menggunakan pendekatan kualitatif dengan paradigma interpretif-eksplanatori yang bertujuan untuk memahami fenomena

keamanan jaringan *wireless* berdasarkan kajian literatur ilmiah. Data penelitian diperoleh melalui metode *Systematic Literature Review* (SLR), yang dilaksanakan secara terstruktur dengan mengacu pada pedoman PRISMA guna menjamin transparansi, konsistensi, dan keterulangan proses analisis. Tahapan analisis data meliputi proses identifikasi, seleksi, dan evaluasi sumber literatur yang relevan dengan topik keamanan jaringan *wireless* dan serangan *Man-in-the-Middle* (MITM). Literatur yang terpilih kemudian dianalisis secara konseptual untuk mengkaji keterkaitan antara teknik serangan MITM, kerentanan pada protokol *wireless*, serta dampaknya terhadap prinsip *Confidentiality*, *Integrity*, dan *Availability* (CIA Triad). Pendekatan analisis ini memungkinkan peneliti untuk memperoleh pemahaman mendalam mengenai pola ancaman dan mekanisme serangan tanpa melakukan pengujian langsung pada sistem jaringan nyata, sehingga penelitian dapat dilakukan secara aman dan sesuai dengan prinsip etika penelitian.

PEMBAHASAN

Hasil implementasi sistem keamanan jaringan *wireless* menunjukkan adanya perbedaan tingkat kerentanan yang signifikan sebelum dan setelah penerapan mekanisme pengamanan. Pada kondisi awal, jaringan *wireless* dioperasikan dengan konfigurasi standar tanpa perlindungan tambahan. Pada tahap ini, lalu lintas komunikasi antara pengguna dan aplikasi web masih dapat diintersepsi oleh pihak lain yang berada dalam segmen jaringan yang sama. Temuan ini mengindikasikan bahwa jaringan wireless dengan tingkat pengamanan minimal sangat rentan terhadap serangan *Man-in-the-Middle* (MITM), khususnya terhadap pelanggaran aspek kerahasiaan data. Penerapan mekanisme enkripsi pada jaringan *wireless* memberikan peningkatan perlindungan yang signifikan. Setelah enkripsi diaktifkan, data yang dipertukarkan antar perangkat tidak lagi dapat dibaca secara langsung oleh pihak yang tidak berwenang. Meskipun lalu lintas jaringan masih dapat terdeteksi, isi komunikasi menjadi tidak dapat diinterpretasikan. Hal ini menunjukkan bahwa enkripsi berperan penting dalam menjaga kerahasiaan informasi serta meminimalkan risiko penyadapan data sensitif selama proses transmisi.

Selain enkripsi, implementasi mekanisme autentikasi yang lebih ketat turut memperkuat keamanan jaringan *wireless.* Pembatasan akses berdasarkan kredensial yang sah terbukti mampu meningkatkan kontrol terhadap perangkat dan pengguna yang terhubung ke jaringan. Dengan demikian, peluang bagi penyerang untuk menyusup ke dalam jaringan dan melakukan serangan MITM dapat dikurangi secara signifikan. Pemantauan lalu lintas jaringan juga memberikan kontribusi penting dalam upaya deteksi dini serangan. Melalui monitoring jaringan, aktivitas anomali seperti perubahan identitas perangkat dan pola komunikasi yang tidak wajar dapat diidentifikasi lebih cepat. Kemampuan deteksi ini memungkinkan administrator jaringan untuk melakukan respons lebih awal sebelum serangan berkembang dan menimbulkan dampak yang lebih besar. Secara keseluruhan, hasil pembahasan menunjukkan bahwa penerapan kombinasi enkripsi, autentikasi yang aman, dan monitoring jaringan mampu meningkatkan tingkat keamanan jaringan *wireless* secara menyeluruh. Pendekatan keamanan berlapis ini tidak hanya efektif dalam mengurangi risiko serangan MITM, tetapi juga

meningkatkan keandalan sistem serta kepercayaan pengguna terhadap jaringan *wireless* yang digunakan.

KESIMPULAN

Berdasarkan hasil analisis dan pembahasan, dapat disimpulkan bahwa jaringan *wireless* memiliki tingkat kerentanan yang lebih tinggi terhadap serangan *Man-in-the-Middle* (MITM) dibandingkan jaringan berbasis kabel. Sifat media transmisi nirkabel yang terbuka memungkinkan pihak yang tidak berwenang untuk mengakses dan mengintersepsi lalu lintas komunikasi apabila tidak dilengkapi dengan sistem keamanan yang memadai. Analisis terhadap mekanisme serangan MITM menunjukkan bahwa penyerang dapat menyusup di antara pengguna dan aplikasi web tanpa terdeteksi, sehingga berpotensi melakukan penyadapan dan manipulasi data. Serangan MITM terbukti mengancam prinsip *Confidentiality* dan *Integrity*, serta berpotensi mengganggu *Availability* layanan jaringan. Hasil implementasi sistem keamanan menunjukkan bahwa penerapan enkripsi yang kuat, mekanisme autentikasi yang aman, dan monitoring jaringan secara berlapis mampu menurunkan risiko terjadinya serangan MITM secara signifikan. Setelah penerapan mekanisme keamanan tersebut, data yang ditransmisikan tidak lagi dapat diinterpretasikan oleh pihak yang tidak berwenang, serta akses terhadap jaringan menjadi lebih terkontrol. Dengan demikian, penerapan kombinasi mekanisme keamanan yang tepat merupakan faktor penting dalam meningkatkan keamanan jaringan *wireless*. Keamanan jaringan tidak hanya ditentukan oleh teknologi yang digunakan, tetapi juga oleh konfigurasi sistem yang benar serta tingkat kesadaran pengguna terhadap pentingnya perlindungan informasi.

DAFTAR PUSTAKA

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. *IEEE Communications Surveys & Tutorials, 18*(3), 2027–2051. https://doi.org/10.1109/COMST.2016.2548426

Creswell, J. W. (2018). *Qualitative inquiry and research design: Choosing among five approaches* (4th ed.). SAGE Publications. https://us.sagepub.com/en-us/nam/qualitative-inquiry-and-research-design/book246896

Forouzan, B. A. (2017). *Data communications and networking* (5th ed.). McGraw-Hill Education. https://www.mheducation.com/highered/product/data-communications-networking-forouzan/M9780073376226.html

Gast, M. (2018). *802.11 wireless networks: The definitive guide* (2nd ed.). O'Reilly Media. https://www.oreilly.com/library/view/80211-wireless-networks/9781449339526/

ISO/IEC. (2022). *ISO/IEC 27001: Information security management systems*. International Organization for Standardization. https://www.iso.org/standard/27001

Kurose, J. F., & Ross, K. W. (2021). *Computer networking: A top-down approach* (8th ed.). Pearson Education. https://www.pearson.com/en-us/subject-catalog/p/computer-networking-a-top-down-approach/P200000003295

Mallik, A. (2019). Man-in-the-middle attack: Understanding in simple words. *Cyber Security Review, 3*(2), 77–92. https://www.researchgate.net/publication/334600018_Man-in-the-Middle_Attack_Understanding_in_Simple_Words

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2015). Preferred reporting items for systematic reviews and meta-analyses (PRISMA). *PLoS Medicine, 6*(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097

NIST. (2020). *Guide to wireless network security (Special Publication 800-153)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

Stallings, W. (2018). *Network security essentials: Applications and standards* (6th ed.). Pearson Education. https://www.pearson.com/en-us/subject-catalog/p/network-security-essentials-applications-and-standards/P200000003321

Tanenbaum, A. S., & Wetherall, D. J. (2021). *Computer networks* (6th ed.). Pearson Education. https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000003296